

**Commonwealth of Virginia  
Department of Juvenile Justice  
Information Security Agreement**

As a user of the Department of Juvenile Justice (DJJ) distributed network, I understand and agree to abide by the following terms that govern my access to and use of the data processing services:

1. Access is granted to me by DJJ as a necessary privilege in order to perform authorized job functions for which I am currently employed.
2. I acknowledge that the data contained in and accessed using DJJ information systems and network is the property of the Commonwealth of Virginia.
3. Although I have access to data, I shall not read, disclose, provide, or otherwise make available, in whole or in part, such information other than to those to whom such disclosure is authorized by the Code of Virginia, Regulation or Policy, and who have a need to know. Such disclosure shall be in confidence for purposes specifically related to the business of DJJ and the Commonwealth of Virginia.
4. I agree that my obligations with respect to the confidentiality and security of all information disclosed to me shall survive the termination of any agreement or relationship with DJJ.
5. I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as login IDs or passwords) for any purpose other than those required to perform my authorized employment functions.
6. I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so by the Agency Head in writing or the Information Security Officer (ISO), and I will not use any access mechanism that has not been expressly assigned to me.
7. I agree that login IDs and passwords are not to be shared or disclosed under any circumstances. There is no exception to this.
8. I acknowledge that all network traffic, including, but not limited to, email, Internet, and LAN communications shall be subject to electronic monitoring; and thus I shall have no expectation of privacy.
9. I agree to abide by all applicable DJJ policies, procedures, standards, directives, and practices that relate to the security of DJJ computer systems and the data contained therein.
10. I shall take all appropriate action to ensure the protection, confidentiality and security of information and automated systems. I will perform my duties with quality and integrity, in a professional manner, and in keeping with established standards. I will report all violations of information security immediately to the Information Security Officer (ISO) at (804)-786-1606 or other backup designated by the ISO.

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. A failure to sign this agreement will result in the suspension of all network access privileges, and may as a result lead to the termination of my employment with this agency.

I further acknowledge that the Department will investigate alleged or suspected violations of this agreement and will suspend service or access to users with or without notice when necessary to protect the operation or integrity of the state communications infrastructure or connected networks.

I further acknowledge that users who violate these guidelines are subject to immediate loss of Network access and other computer resources. In addition, employees may be subject to disciplinary action up to and including discharge, under the Commonwealth's Standards of Conduct; and contractors assigned to or working for the agency may be subject to administrative and contractual sanctions. Criminal or civil action may be initiated in appropriate instances.

I have been given a copy of DJJ Administrative Directive 02-002.2, "Internet Access and Computer Utilization" and I understand it is my responsibility to read and abide by this policy, even if I do not agree with it. If I have any questions about the directive, I understand that I need to ask my supervisor for clarification.

I further certify that I understand that the granting of, or continuation of, access privileges is dependent upon successful completion in the allocated time of designated security awareness training.

_____ Employee Name (Please Print)	_____ Date
_____ Employee Signature	_____ Last 4 digits of SSN
_____ Office Location	_____ Division Name